A NOTE ON DIVISIBLE POINTS OF CURVES

M. BAYS AND P. HABEGGER

Abstract. Let C be an irreducible algebraic curve defined over a number field and inside an algebraic torus of dimension at least 3. We partially answer a question posed by Levin on points on C for which a non-trivial power lies again on C. Our results have connections to Zilber's Conjecture on Intersections with Tori and yield to methods arising in transcendence theory and the theory of o-minimal structures.

1. Introduction

Let C_1 and C_2 be irreducible algebraic curves in the algebraic torus $\mathbf{G}_m^N$ with $N \geq 3$. Aaron Levin asked what can be said of points x on C_1 for which there is $n \geq 2$ such that x^n is on C_2. In this paper we give a partial answer to Levin's question in the case $C_1 = C_2$.

The maximal compact subgroup of the algebraic torus is the real torus

$$\mathbf{T} = \{(x_1, \ldots, x_N) \in \mathbf{G}_m^N(\mathbf{C});\ |x_1| = \cdots = |x_N| = 1\}.$$

It is convenient to call a translate of an algebraic subgroup of $\mathbf{G}_m^N$ a *coset* (of $\mathbf{G}_m^N$). Moreover, a *torsion coset* (of $\mathbf{G}_m^N$) is a coset containing an element of finite order. Torsion cosets are precisely irreducible components of algebraic subgroups of $\mathbf{G}_m^N$. We call a coset or torsion coset *proper* if it is not equal to $\mathbf{G}_m^N$.

Say $C \subset \mathbf{G}_m^N$ is an algebraic curve defined over a number field F. If $\sigma : F \to \mathbf{C}$ is a field embedding, then C_σ is the curve defined over $\mathbf{C}$ by polynomials obtained from applying σ to polynomials defining C. Let $\overline{\mathbf{Q}}$ be a fixed algebraic closure of $\mathbf{Q}$; we take number fields to be subfields of $\overline{\mathbf{Q}}$.

Theorem 1. *Let $N \geq 3$ and let $C \subset \mathbf{G}_m^N$ be an irreducible closed algebraic curve defined over a number field F. We assume that C is not contained in a proper torsion coset of $\mathbf{G}_m^N$. Let us also assume that $C_\sigma(\mathbf{C}) \cap \mathbf{T}$ is finite for some $\sigma : F \to \mathbf{C}$. Then $C(\overline{\mathbf{Q}})$ contains only finitely many points x with $x^n \in C(\overline{\mathbf{Q}})$ for some $n \geq 2$.*

The condition $N \geq 3$ is natural for this type problem on unlikely intersections, cf. Zannier's book [18] where Levin's question appears in print. If x is as in (i) of the theorem, then (x, x^n) is contained in the surface $C \times C$. However, it is also in an algebraic subgroup of codimension $N > \dim(C \times C)$. Our result gives new evidence towards Zilber's Conjecture [20] on intersections with tori for surfaces in $\mathbf{G}_m^N$. The class of degenerate subvarieties, of which $C \times C$ is a member, has eluded recent progress by Maurin [11] and the second author [8] towards this conjecture. Degenerate subvarieties are defined in Maurin's work [11]; an equivalent definition is $(C \times C)^{\mathrm{oa}} = \emptyset$ in Bombieri, Masser, and Zannier's notation, cf. [8].

However, the finiteness condition on $C_\sigma(\mathbf{C}) \cap \mathbf{T}$ does not appear in the theory of unlikely intersections, and it would follow from Zilber's conjecture that the condition is

not necessary. Any curve that is also a torsion coset intersects $\mathbf{T}$ in the infinite set of its points of finite order. There are however also algebraic curves that are not contained in a proper torsion coset but that intersect $\mathbf{T}$ in infinitely many points. An example is

$$\left\{ \left(x, \frac{x-2}{2x-1} \right);\ x \in \mathbf{C} \smallsetminus \{1/2\} \right\}.$$

Indeed, if $|x| = 1$ then $|x-2| = |2x-1|$.

More generally, the birational map $\mathbf{C} \to \mathbf{C}; z \mapsto \frac{z-1}{iz+1}$ maps the unit circle onto $\mathbf{P}(\mathbf{R}) = \mathbf{R} \cup \{\infty\}$, and so sets up a bijective correspondence between curves in $\mathbf{G}_m^N$ which have infinite intersection with $\mathbf{T}$ and curves in $\mathbf{C}^N$ whose closure in $\mathbf{P}(\mathbf{C})^N$ have infinite intersection with $\mathbf{P}(\mathbf{R})^N$. So examples are plentiful.

The intersection of the line $x_1 + x_2 = 1$ with $\mathbf{T}$, however, consists precisely of the two points $\{(\exp(\pm 2\pi i/6), \exp(\mp 2\pi i/6)\}$.

Corvaja, Masser, and Zannier [5] recently proved finiteness results when intersecting an algebraic curve with the maximal compact subgroup of certain commutative algebraic groups.

Our proof involves the Theorem of Pila-Wilkie [13] which is playing an increasingly important role in diophantine problems revolving around unlikely intersections. Zannier proposed to use this tool to give a new proof of the Manin-Mumford Conjecture for abelian varieties in joint work with Pila [14]. Maurin's work [11] relies on a generalized Vojta inequality due to Rémond. Our work uses an earlier variant of this result also due to Rémond [15], which almost immediately implies (see Lemma 6) that x as in Theorem 1 has height bounded only in terms of C. The new ingredient in our work is the use of Baker's inequality on linear forms in logarithms. Its effect is to obtain a lower bound for the degree of x from the height bound obtained from Rémond's result. We refer to Baker and Wüstholz's estimate [2], which is completely explicit.

Using a p-adic version of linear forms in logarithms due to Bugeaud and Laurent we also obtain the following partial result for curves that do not satisfy the finiteness condition in Theorem 1.

Let S be a set of rational primes. A tuple $(x_1, \ldots, x_N)$ of algebraic numbers is called S-integral if $\max\{|x_1|_v, \ldots, |x_N|_v\} \le 1$ for all finite places v of $\mathbf{Q}(x_1, \ldots, x_N)$ with residue characteristic outside of S.

Theorem 2. *Let $N \ge 3$ and let $C \subset \mathbf{G}_m^N$ be an irreducible closed algebraic curve defined over a number field F. We assume that C is not contained in a proper torsion coset of $\mathbf{G}_m^N$. There is a constant p_0 with the following property. If S is a finite set of rational primes with $\inf S > p_0$, then $C(\overline{\mathbf{Q}})$ contains only finitely many S-integral points x such that $x^n \in C(\overline{\mathbf{Q}})$ for some $n \ge 2$.*

By convention the infimum of the empty set is $+\infty$. So $S = \emptyset$ is allowed and yields a finiteness statement on points whose coordinates are algebraic integers.

The paper is organized as follows. In the next section we set up common notation used throughout the article. The third section contains an elementary metric argument which is used in connection with Baker-type estimates in section 4. In section 5 we bound from below the size of Galois orbits and section 6 contains the arguments from o-minimality. Finally, both theorems are proved simultaneously in section 7.

Bays was partially supported by the Agence Nationale de Recherche [MODIG, Project ANR-09-BLAN-0047], and both authors thank Zoé Chatzidakis and the ANR for supporting Habegger's invitation to Paris in Summer of 2011, where the authors worked together on this problem. Habegger is also grateful to Yann Bugeaud for answering questions in connection with linear forms in p-adic logarithms.

2. Notation

By a place v of a number field K we mean an absolute value that is, when restricted to $\mathbf{Q}$, either the complex absolute value or a p-adic absolute value for some prime p. A non-Archimedean place is called finite and the others are called infinite. We let K_v denote a completion of K with respect to v and, by abuse of notation, $\mathbf{Q}_v$ a completion of $\mathbf{Q}$ with respect to the restriction of v.

For purposes of bookkeeping it is convenient to work with height functions. We recall here the absolute logarithmic Weil height used throughout the article. Let $x \in \overline{\mathbf{Q}}$. There is a unique irreducible polynomial $P \in \mathbf{Z}[X]$ with $P(x) = 0$ and positive leading term a_0. We define the height x as

$$h(x) = \frac{1}{\deg P} \log \left(a_0 \prod_{\substack{z \in \mathbf{C} \\ P(z)=0}} \max\{1, |z|\} \right).$$

If K is a number field containing x, then the height $h(x)$ defined above is

$$\frac{1}{[K : \mathbf{Q}]} \sum_v d_v \log \max\{1, |x|_v\} \tag{1}$$

where v ranges over places of K, and $d_v = [K_v : \mathbf{Q}_v]$, the degree of the corresponding field extension of the completions. Equivalently,

$$h(x) = \frac{1}{[K : \mathbf{Q}]} \sum_p \sum_{\sigma : K \hookrightarrow \mathbf{C}_p} \log \max\{1, |\sigma(x)|_p\} \tag{2}$$

where p ranges over ∞ and the primes, $\mathbf{C}_\infty = \mathbf{C}$, and $\mathbf{C}_p$ is a completion of an algebraic closure of the field of p-adic numbers if $p \neq \infty$.

The height of a tuple $x = (x_1, \ldots, x_N) \in \overline{\mathbf{Q}}^N$ is

$$h(x) = \max\{h(x_1), \ldots, h(x_N)\}.$$

The exponential height of x is $H(x) = \exp(h(x))$.

3. A Metric Argument

The following elementary lemma is well-known and sometimes proved using Puiseux series. We have decided to include an elementary argument that essentially relies only on the triangle inequality.

We let $\langle \cdot, \cdot \rangle$ denote the standard inner product on $\mathbf{R}^2$ and $\| \cdot \|$ the Euclidean norm. If $i \in \mathbf{R}^2$ we use i_1 and i_2 to denote its coordinates. A non-zero vector $i \in \mathbf{Z}^2$ is called reduced if i_1, i_2 are coprime and if either $i_1 \geq 1$ or $i = (0, 1)$. We note that two reduced vectors are linearly dependent if and only if they are equal.

If K is a field then $K^\times$ is its multiplicative group. For this section we suppose that K is algebraically closed and endowed with an absolute value $|\cdot|: K \to \mathbf{R}$.

Lemma 1. *Suppose $P \in K[X^{\pm 1}, Y^{\pm 1}]$ is a Laurent polynomial with at least 2 non-zero terms. We set $D = \max_{p_i p_{i'} \neq 0} \|i - i'\|$ and let $\sigma + 1 \geq 2$ denote the number of non-zero terms of P if $|\cdot|$ is Archimedean and $\sigma = 1$ otherwise. There exists a finite set $\Sigma \subset K^\times$ depending only on P with the following property. Let $x_1, x_2 \in K^\times$ with $P(x_1, x_2) = 0$ satisfy $\|L\| > 16D^2(\log\sigma + \max_{p_i p_{i'} \neq 0} \log|p_i/p_{i'}|)$ where $L = (\log|x_1|, \log|x_2|) \in \mathbf{R}^2$. Then there is $\alpha \in \Sigma$ and a reduced $j \in \mathbf{Z}^2$ with $\|j\| \leq D$ such that*

$$x_1^{j_1} x_2^{j_2} = \alpha \quad \text{or} \quad \log|x_1^{j_1} x_2^{j_2} - \alpha| \leq -\frac{1}{16D^2}\|L\|.$$

Proof. The set Σ and the value of $c > 0$ will be determined during the argument. Say (x_1, x_2) is as in the hypothesis. We write $P = \sum_i p_i X^{i_1} Y^{i_2}$. After possibly dividing P by some non-zero term $p_i X^{i_1} Y^{i_2}$ we may suppose that the constant term of P is 1 and $|p_i x_1^{i_1} x_2^{i_2}| \leq 1$ for all $i \in \mathbf{Z}^2$. By abuse of notation we sometimes also write $|\cdot|$ for the standard absolute value on $\mathbf{R}$.

Let us fix a non-zero element i of $\mathbf{Z}^2$ for which $|p_i x_1^{i_1} x_2^{i_2}|$ is maximal.

Then $\langle L, i\rangle \leq -\log|p_i|$ and we will now bound this quantity from below. In the Archimedean case we estimate

$$1 - |p_i x_1^{i_1} x_2^{i_2}| \leq |1 + p_i x_1^{i_1} x_2^{i_2}| = \left|\sum_{i' \neq 0, i} p_{i'} x_1^{i'_1} x_2^{i'_2}\right| \leq \sum_{i' \neq 0, i} |p_{i'} x_1^{i'_1} x_2^{i'_2}| \leq (\sigma - 1)|p_i x_1^{i_1} x_2^{i_2}|$$

by the triangle inequality and the choice of i. Hence $|p_i x_1^{i_1} x_2^{i_2}| \geq \sigma^{-1}$ which is also true in the non-Archimedean case. Therefore, $|\langle L, i\rangle| \leq |\log|p_i|| + \log\sigma < \|L\|/(8D^2)$ by hypothesis. We divide by $\|i\|$ and set $v_1 = i/\|i\|$ to get

$$|\langle L, v_1\rangle| < \frac{\|L\|}{8D^2}. \tag{3}$$

We fix $v_2 \in \mathbf{R}^2$ of norm 1 with $\langle v_1, v_2\rangle = 0$. After multiplying by -1 we may suppose $\langle L, v_2\rangle \geq 0$. We have $\langle L, v_2\rangle^2 = \|L\|^2 - \langle L, v_1\rangle^2$ and use (3) to estimate

$$\langle L, v_2\rangle = |\langle L, v_2\rangle| \geq \frac{\|L\|}{2}. \tag{4}$$

Suppose $i' \in \mathbf{Z}^2$ is written as $\lambda_1 v_1 + \lambda_2 v_2$ with new real coordinates $\lambda_{1,2}$. Then $\lambda_2 = \langle i', v_2\rangle$. But the coordinates of v_2 are up-to sign the coordinates of $v_1 = i/\|i\|$ and so either $\lambda_2 = 0$ or $|\lambda_2| \geq 1/\|i\|$.

Now suppose also $p_{i'} \neq 0$. We claim $\lambda_2 \leq 0$. Indeed, otherwise we would have $\lambda_2 \geq 1/\|i\| \geq 1/D$. Now $0 \geq \log|p_{i'}| + \langle L, i'\rangle$, so $0 \geq \log|p_{i'}| + \lambda_1\langle L, v_1\rangle + \lambda_2\langle L, v_2\rangle$. We remark that $|\lambda_1| = |\langle i', v_1\rangle| \leq \|i'\| \leq D$. Using (3) and (4) yields $0 \geq \log|p_{i'}| - \|L\|/(4D) + \|L\|/(2D) = \log|p_{i'}| + \|L\|/(4D)$. So $\|L\| \leq 4D|\log|p_{i'}||$ which contradicts our hypothesis. Thus $\lambda_2 \leq 0$.

We have $0 = P(x_1, x_2) = A + B$ with

$$A = \sum_{i' = \lambda_1 v_1} p_{i'} x_1^{i'_1} x_2^{i'_2} \quad \text{and} \quad B = \sum_{i' = \lambda_1 v_1 + \lambda_2 v_2,\, \lambda_2 < 0} p_{i'} x_1^{i'_1} x_2^{i'_2}.$$

We first treat the error term B. If it is non-zero, the triangle or ultrametric triangle inequality yields $\log|B| \leq \log\sigma + \max_{\lambda_2 < 0}\{\log|p_{i'}| + \lambda_1\langle L, v_1\rangle + \lambda_2\langle L, v_2\rangle\}$. To treat the

terms in the maximum we use the bounds (3), (4), $|\lambda_1| \leq D$, and $\lambda_2 \leq -1/D$ proved above. Indeed,

$$\log|B| \leq \log\sigma + \max_{i'}\{\log|p_{i'}|\} + \frac{\|L\|}{8D} - \frac{\|L\|}{2D} \leq -\frac{\|L\|}{4D}. \tag{5}$$

Now we consider the main term A to which we associated the polynomial $F = \sum_{i'=\lambda_1 v_1} p_{i'} X^{i'_1} Y^{i'_2}$. We fix a primitive generator j of the rank 1 group $i\mathbf{Q} \cap \mathbf{Z}^2$. Then $j = \mu v_1$ with $\mu \in \mathbf{R}$. We can write $F = \sum_\lambda f_\lambda X^{\lambda j_1} Y^{\lambda j_2}$ where λ runs over integers and the f_λ are certain coefficients of P. We define $G = \sum_\lambda f_\lambda T^\lambda \in K[T^{\pm 1}]$ and with this new Laurent polynomial we have $G(X^{j_1} Y^{j_2}) = F$. Note that 1 is the constant term of G. Say a is the minimal integer such that $T^a G$ is a polynomial. Let us now factor $T^a G = p(T - \alpha_1) \cdots (T - \alpha_d)$ where $p \neq 0$ is some coefficient of P. We remark that $\alpha_1, \ldots, \alpha_d$ do not vanish and come from a finite set depending only on P.

For brevity we write $z = x_1^{j_1} x_2^{j_2} \in K^\times$. Then $p(z - \alpha_1) \cdots (z - \alpha_d) = z^a G(z) = z^a F(x_1, x_2) = -z^a B$. Without loss of generality we may assume $|z - \alpha_1| \leq |z - \alpha_k|$ for $1 \leq k \leq d$. So $|z - \alpha_1|^d \leq |p|^{-1} |z|^a |B|$.

If $z = \alpha_1$ then we are in the first case of the conclusion. Else we take the logarithm and use (5) to estimate

$$d \log|z - \alpha_1| \leq -\log|p| + a\log|z| + \log|B| \leq |\log|p|| + |a\log|z|| - \frac{\|L\|}{4D}. \tag{6}$$

We conclude by first bounding $|a\log|z|| = |a\mu\langle L, v_1\rangle|$. The inequality $|a\mu| = |a\mu|\|v_1\| = \|aj\| \leq D$ and (3) imply $|a\log|z|| \leq \|L\|/(8D)$. Moreover, $|\log|p|| \leq \|L\|/(16D)$. Inserting these two inequalities into (6) yields $d\log|z - \alpha_1| \leq -\|L\|/(16D)$. The lemma follows since $d \leq D$. $\square$

Remark 1. *Note that in the case that $|\cdot|$ is non-Archimedean and all coefficients of P have trivial absolute value, the condition on $\|L\|$ in Lemma 1 is just that it is non-trivial. We will use this in our proof of Theorem 2 below.*

Let us also remark that a qualitative version of Lemma 1, which does not give this information needed for Theorem 2 but which suffices for our uses in proving Theorem 1, admits a proof using the model theory of valued fields. We sketch this here.

Let K be an algebraically closed field with an absolute value $|\cdot| : K \to \mathbf{R}$.

Define $v : K \to \mathbf{R} \cup \{\infty\}$; $v(x) := -\log|x|$. This is a valuation if and only if $|\cdot|$ is non-Archimedean. Consider the two-sorted structure $\langle \langle K; +, \cdot \rangle, \langle \mathbf{R}; +, < \rangle; v \rangle$ consisting of the field K, the ordered group $\mathbf{R}$, and the map v.

Let $({}^*K, {}^*\mathbf{R})$ be an elementary extension, extending v to a map $v : {}^*K \to {}^*\mathbf{R} \cup \{\infty\}$. Let $\mathcal{O} := \{x \in {}^*K \mid \exists n \in \mathbb{N}.\ v(x) > -n\}$. Then $\mathcal{O}$ is a local ring, since $v(x^{-1}) = -v(x)$. Let v' be the corresponding valuation, and let res *be the corresponding residue map. Note that the restriction of* res *to K is an embedding.*

(In the case that $|\cdot|$ is non-Archimedean, v' is the coarsening of v obtained by quotienting the value group $v({}^*K)$ by the convex hull of the standard value group $v(K)$. In the Archimedean case with $K = \mathbf{C} = \mathbf{R} + i\mathbf{R}$, we can consider res *as being induced by the standard part map ${}^*\mathbf{R} \to \mathbf{R}$)*

Now let $C \subseteq \mathbb{G}_m^n$ be a curve defined over K, and let $x \in C({}^*K)$. Suppose $||v'(x)|| := \max_i |v'(x_i)| > 0$. By the transcendental valuation inequality [7, Theorem 3.4.3], *we have the following inequality on transcendence degrees of fields and dimensions of $\mathbb{Q}$-vector*

spaces:

$$1 = \operatorname{trd}(K(x)/K) \geq \dim_{\mathbb{Q}}(v'(K(x))/v'(K)) + \operatorname{trd}(\operatorname{res}(K(x))/\operatorname{res}(K))$$

But $v'(K) = 0$ *and* $v'(x) \neq 0$*, so we deduce* $\dim_{\mathbb{Q}}(v'(K(x))) = 1$ *and* $\operatorname{res}(K(x)) = \operatorname{res}(K)$*. So say* $\theta : \mathbb{G}_m^n \to \mathbb{G}_m^{n-1}$ *is an algebraic epimorphism such that* $v'(\theta(x)) = 0$*. Then* $\operatorname{res}(\theta(x)) = \operatorname{res}(\alpha)$ *for some* $\alpha \in \mathbb{G}_m^{n-1}(K)$*.*

Now let $\beta := \theta(x) - \alpha$*. Then* $\operatorname{res}(\beta) = 0$*, so* $v'(\beta) \neq 0$*, so since* $\dim_{\mathbb{Q}}(v'(K(x))) = 1$*, if* $\beta \neq 0$ *we have* $||v'(\beta)|| = q||v'(x)||$ *for some* $q \in \mathbb{Q}$*,* $q > 0$*.*

Applying the compactness theorem of first-order logic, it follows that there exist finitely many pairs (θ, α) *of algebraic epimorphisms*

$$\theta : \mathbb{G}_m^n \to \mathbb{G}_m^{n-1}$$

and points $\alpha \in \mathbb{G}_m^{n-1}(K)$*, and there exist* $q \in \mathbb{Q}$*,* $q > 0$ *and* $B > 0$ *such that for any* $x \in K$ *if* $||v(x)|| := \max_i(|v(x_i)|) > B$ *then for one of the finitely many pairs* (θ, α)*,*

$$||v(\theta(x) - \alpha)|| > q||v(x)||.$$

4. Baker's Linear Forms in Logarithms

In order to prove our theorems, we must treat Archimedean and non-Archimedean places separately. We begin by proving a technical lemma for the latter. Its proof is elementary.

Lemma 2. *For* F *a number field,* $\alpha \in F^\times$*,* p *a prime, and* $B \geq 1$ *there is a constant* $c > 0$ *with the following property. Say* $z \neq 0$ *is algebraic over* F *and not a root of unity such that* z *and* α *are multiplicatively dependent. We also suppose that* $h(z) \leq B$ *and that* $|z - 1|_v < 1$ *for some finite place* v *of* $F(z)$ *with residue characteristic* p*. Then* $[F(z) : F] + \log n \geq -c \log |z^n - \alpha|_v$ *for all* $n \geq 2$ *for which* $z^n\alpha^{-1}$ *has infinite order.*

Proof. In this lemma, the constants involved in Vinogradov symbols $\ll, \gg$ depend only on F, α, p, and B. Let e be the ramification index of v above p.

The setup and the ultrametric triangle inequality imply $|z|_v = 1$.

Let us suppose first that α has finite order, say $m \ll 1$. We fix the integer $t \geq 0$ with $p^{t-1} \leq e/(p-1) < p^t$. The corollary after lemme 3 [4] yields $|z^{p^t} - 1|_v < p^{-1/(p-1)}$. Hence z^{p^t} and lies in the image of the domain of convergence of the p-adic exponential $\exp(x) = \Sigma_i x^i/i!$; cf. Chapter II.5 [12]. It follows that $|z^{kp^t} - 1|_v = |k|_v|z^{p^t} - 1|_v$ for any $k \in \mathbf{N}$.

Hence we have

$$|mn|_v|z^{p^t} - 1|_v = |z^{mnp^t} - 1|_v \leq |z^{mn} - 1|_v \leq |z^n - \alpha|_v$$

and note that the very left-hand side is non-zero. Using $|mn|_v \geq 1/(mn)$ and taking the ordinary logarithm yields

$$\log |z^{p^t} - 1|_v \leq \log(mn) + \log |z^n - \alpha|_v. \tag{7}$$

By the local nature of our height (1), and since $d_v \geq e$, we have $-e \log |z^{p^t} - 1|_v \leq [F(z) : \mathbf{Q}]h((z^{p^t} - 1)^{-1})$. Basic height properties, $h(z) \leq B$, and $p^t \leq ep/(p-1) \leq 2e$ now imply

$$e \log |z^{p^t} - 1|_v \geq -[F(z) : \mathbf{Q}]h(z^{p^t} - 1) \geq -[F(z) : \mathbf{Q}](\log 2 + p^t B) \gg -[F(z) : F]e.$$

The lemma follows if α has finite order after cancelling e and using (7).

Now we assume that α has infinite order. There is a unique reduced $(k,l) \in \mathbf{Z}^2$ such that $z^k\alpha^l = \zeta$ is a root of unity. We note that $kl \neq 0$ and that any pair $(k',l') \in \mathbf{Z}^2$ for which $z^{k'}\alpha^{l'}$ has finite order is an integral multiple of (k,l). To complete the proof we may assume $|z^n - \alpha|_v < p^{-1/(p-1)}$. This implies $|\alpha|_v = 1$ and this time we fix $m \in \mathbf{N}$ such that $|\alpha^m - 1|_v < p^{-1/(p-1)}$ and $m \ll 1$. Thus

$$|\zeta^n - \alpha^{nl+k}|_v = |(\zeta\alpha^{-l})^n - \alpha^k|_v = |z^{nk} - \alpha^k|_v \leq |z^n - \alpha|_v < p^{-1/(p-1)}$$

and passing to the m-th power gives

$$|\zeta^{mn} - \alpha^{m(nl+k)}|_v \leq |z^n - \alpha|_v < p^{-1/(p-1)}. \tag{8}$$

But $|\alpha^{m(nl+k)} - 1|_v < p^{-1/(p-1)}$ holds as well. We use the ultrametric inequality to obtain $|\zeta^{mn} - 1|_v < p^{-1/(p-1)}$. The only root of unity that is p-adically closer to 1 than $p^{-1/(p-1)}$ is 1 itself. So $\zeta^{mn} = 1$ and therefore $|\alpha^{m(nl+k)} - 1|_v \leq |z^n - \alpha|_v$ by (8). By our choice of m the element α^m is in the image of the domain of convergence of the p-adic exponential. So as above, we can estimate

$$|nl + k|_v |\alpha^m - 1|_v = |\alpha^{m(nl+k)} - 1|_v \leq |z^n - \alpha|_v,$$

so

$$|nl + k|_v \ll |z^n - \alpha|_v$$

since α is not a root of unity. We remark that the left-hand side is non-zero. Indeed, $nl + k \neq 0$ since z^n/α is not a root of unity

Using $|nl + k|_v \geq |2nlk|^{-1}$ we get $|nlk| \gg |z^n - \alpha|_v^{-1}$. So $\log|nlk| \gg -\log|z^n - \alpha|_v$ because $|nlk| \geq n \geq 2$. The heights satisfy $kh(z) = |l|h(\alpha)$ since $z^k = \zeta\alpha^{-l}$. But $\alpha \neq 0$ is not a root of unity. So $h(\alpha) > 0$ by Kronecker's Theorem and therefore $|l| \ll k$. This leaves us with

$$\log(nk) \gg -\log|z^n - \alpha|_v \tag{9}$$

and to complete the proof we need to control k.

The lemma follows immediately if $k = 1$. Else $k \geq 2$ and Dirichlet's Theorem from diophantine approximation provides us with integers k' and l' such that $1 \leq k' \leq k/2$ and $|k'l - l'k| \leq 2$. So $h(z^{k'}\alpha^{l'}) = |k'l/k - l'|h(\alpha) \leq 2h(\alpha)/k$. On the other hand, $z^{k'}\alpha^{l'}$ cannot have finite order since $1 \leq k' < k$. By a weak version of Dobrowolski's Theorem [6] we have $h(z^{k'}\alpha^{l'}) \gg [F(z) : F]^{-2}$. So $k \ll [F(z) : F]^2$. The lemma follows from this inequality in combination with (9). $\square$

In the following lemma, we apply Baker's technique of estimating linear forms in logarithms. In the Archimedean case we use the explicit estimates of Baker and Wüstholz [2], and in the non-Archimedean case we use a p-adic version obtained by Bugeaud and Laurent [4].

It is useful to define $L : \mathbf{G}_m^N(\mathbf{C}) \to \mathbf{R}^N$ by $L(x_1, \ldots, x_N) = (\log|x_1|, \ldots, \log|x_N|)$.

Lemma 3. *Let F be a number field and $C \subset \mathbf{G}_m^2$ a geometrically irreducible algebraic curve defined over F. We suppose that C is not contained in a proper coset of $\mathbf{G}_m^2$. Let $B \geq 1$. Let $x = (x_1, x_2) \in C(\overline{\mathbf{Q}})$ with $h(x) \leq B$ and $x^n \in C(\overline{\mathbf{Q}})$ where $n \geq 2$ is an integer.*

(i) *Say $\sigma : F(x) \to \mathbf{C}$ is an embedding and $L = L(\sigma(x))$ then*

$$[F(x) : F] \geq c \left(\frac{n}{\log n} \|L\| \right)^{1/6} \tag{10}$$

where $c > 0$ depends only on C and B.

(ii) *Say v is a finite place of the number field $F(x)$ lying above a rational prime that is sufficiently large with respect to C. If $(\log |x_1|_v, \log |x_2|_v) \neq 0$, then*

$$[F(x) : F] \geq cn^{1/9} \tag{11}$$

where $c > 0$ depends only on $C, B,$ and the residue characteristic of v.

Proof. For part (i) the constant c is meant to be sufficiently small with respect to B, C, and F. It will be fixed throughout the proof. The constants implicit in $\ll$ and $\gg$ below are positive and depend only on B, C, and F. They are independent of x and c. Clearly, we may assume

$$n\|L\| > c^{-6} \log n$$

as the conclusion (10) is immediate otherwise.

The conclusion of Lemma 1 applied to the point $(\sigma(x_1)^n, \sigma(x_2)^n)$ is

$$\log |z^n \beta - 1| \ll -n\|L\| \quad \text{where} \quad z = \sigma(x_1^{j_1} x_2^{j_2}), \tag{12}$$

for algebraic $\beta \in \mathbf{C}^\times$ and $j \in \mathbf{Z}^2 \smallsetminus \{0\}$, both coming from a finite set depending only on C. After decreasing c we may assume that the left-hand side of (12) is less than -1.

Let $l_1, l_2 \in \mathbf{C}$ be choices of logarithms of z and β. That is, $e^{l_1} = z$ and $e^{l_2} = \beta$. Some elementary calculus yields

$$\log |\Lambda| \ll -n\|L\| \quad \text{with} \quad \Lambda = nl_1 + l_2 + 2\pi i k$$

where k is an appropriate integer with $|k| \ll n$.

In order to apply Baker's theory to bound $|\Lambda|$ from below we must first treat the case $\Lambda = 0$, so $z^n = \beta^{-1}$.

If β is a not a root of unity, then z is not one either. The same weak version of Dobrowolski's Theorem as is used in Lemma 2 implies

$$\frac{h(\beta)}{n} = h(z) \gg \frac{1}{[\mathbf{Q}(z) : \mathbf{Q}]^2} \gg \frac{1}{[F(z) : F]^2} \geq \frac{1}{[F(x) : F]^2}. \tag{13}$$

Hence $n \ll [F(x) : F]^2$ because β is from a finite set depending only on P. The definition of the height implies $\|L\| \ll [\mathbf{Q}(x) : \mathbf{Q}] h(x)$. But $h(x) \leq B$ by hypothesis, so $\|L\| \ll [\mathbf{Q}(x) : \mathbf{Q}] \ll [F(x) : F]$. We may thus bound

$$\frac{n}{\log n} \|L\| \ll [F(x) : F] n \ll [F(x) : F]^3 \tag{14}$$

and the lemma follows in this case.

But what if β is a root of unity? Then some positive power of z^n is 1. Hence x^n is contained in a proper algebraic subgroup of $\mathbf{G}_m^2$. But this is also a point on C. Over 10 years ago Bombieri, Masser, and Zannier [3] proved that $h(x^n)$ is bounded from above by a constant depending only on C. Here it is essential that C is not contained in a

proper coset. So $h(x) \ll 1/n$. By height inequalities similar to those used above we find $\|L\| \ll [F(x):F]h(x) \ll [F(x):F]/n$ and therefore

$$\frac{n}{\log n}\|L\| \ll [F(x):F].$$

We have proved (10) in the case $\Lambda = 0$.

Let us now assume $\Lambda \neq 0$; we apply results on linear forms in logarithms. An explicit version due to Baker and Wüstholz [2] yields

$$\log|\Lambda| \gg -[\mathbf{Q}(x):\mathbf{Q}]^6(\log A_1)(\log A_2)(\log A_3)\log n$$

where A_1, A_2, A_3 are bounded in terms of the heights of $x_1^{j_1}x_2^{j_2}$ and β. But $h(x_1^{j_1}x_2^{j_2}) \leq |j_1|h(x_1) + |j_2|h(x_2) \ll 1$ and so we may streamline the inequality from above to get

$$\log|\Lambda| \gg -[\mathbf{Q}(x):\mathbf{Q}]^6 \log n.$$

We conclude by comparing this with the upper bound for $\log|\Lambda|$ derived above, since this gives $\frac{n}{\log n}\|L\| \ll [\mathbf{Q}(x):\mathbf{Q}]^6$ and thus completes the proof of (i).

Say v is as in (ii) and let e be the ramification index of v above the rational prime.

Say C is cut out by a polynomial P. We may suppose that all non-zero coefficients of P and all α provided by Lemma 1 (which do not depend on v) lie in F and have v-adic absolute value 1.

In the proof of part (ii) we allow the constants in $\ll$ and $\gg$ to also depend on the residue characteristic of v. In this non-Archimedean case we only assume $L = (\log|x_1|_v, \log|x_2|_v) \neq 0$ which implies the lower bound $\|L\| \geq 1/e$. In order to complete the proof we may assume $e < n^{1/2}$ since $e \geq n^{1/2}$ implies $[F(x):F] \gg e \geq n^{1/2}$.

By Lemma 1 there are reduced vectors $j, j' \in \mathbf{Z}^2$ with

$$\log|z^n - \alpha|_v \ll -\frac{n}{e} \leq -n^{1/2} \tag{15}$$

and $|z' - \alpha'|_v < 1$ where $z = x_1^{j_1}x_2^{j_2}$, $z' = x_1{}^{j_1'}x_2{}^{j_2'}$, and α, α' depend only on P.

Since $|\alpha|_v = |\alpha'|_v = 1$ we find $|z|_v = |z'|_v = 1$. Moreover, $L \neq 0$ so the two equalities

$$j_1 \log|x_1|_v + j_2 \log|x_2|_v = 0 \quad \text{and} \quad j_1' \log|x_1|_v + j_2' \log|x_2|_v = 0$$

imply that j and j' are linearly dependent. Hence $j = j'$ because they are reduced. In particular, $z = z'$. There is $g \ll 1$ with $|\alpha'^g - 1|_v < 1$ and it satisfies $|z^g - 1|_v < 1$ because $|z - \alpha'|_v < 1$.

The exponent g plays an important role in Bugeaud and Laurent's work [4]. Before applying their théorème 3 to z and α' we must first treat the case where these elements are multiplicatively dependent.

If this is the case and if both z and z^n/α have infinite order we may apply Lemma 2. In this case part (ii) follows with ample margin because of (15). If z has finite order, then $e\|L\| \ll [F(x):F]/n$ as in the Archimedean case by appealing to the Theorem of Bombieri, Masser, and Zannier. But $e\|L\| \geq 1$ and hence $[F(x):F] \gg n$, which is better than the claim. If z^n/α has finite order and z has infinite order, then α has infinite order and $nh(z) = h(\alpha) \ll 1$. We can argue as near (13) using a height lower bound to again obtain $[F(x):F] \gg n^{1/2}$.

Finally, suppose z and α' are multiplicatively independent. Then Bugeaud and Laurent's result [4, Théorème 2] implies

$$-\log|z^n-\alpha|_v \ll [F(z):F]^4(\log n)^2.$$

We combine this inequality with (15) to conclude the proof. □

5. Galois Orbits

Let $N\geq 2$. Throughout this section F is a number field and, if not stated otherwise, $C\subset \mathbf{G}_m^N$ is a geometrically irreducible algebraic curve defined over F. The following lemma is a weak equidistribution statement on curves

Lemma 4. *Suppose that C is not contained in a proper coset of $\mathbf{G}_m^N$ and that there exists an embedding $\sigma_0:F\to\mathbf{C}$ such that the curve $C_{\sigma_0}(\mathbf{C})\cap\mathbf{T}$ is finite. For any $B\geq 1$ there exists $\epsilon>0$ with the following property. For $x\in C(\overline{\mathbf{Q}})$ with $h(x)\leq B$ and $[F(x):F]\geq (2\#C_{\sigma_0}(\mathbf{C})\cap\mathbf{T})^N$ there is an embedding $\sigma:F(x)\to\mathbf{C}$ extending σ_0 such that*

$$\|L(\sigma(x))\|\geq\epsilon.$$

Proof. By hypothesis, the intersection $C_{\sigma_0}(\mathbf{C})\cap\mathbf{T}$ is finite. If the intersection is empty, the lemma is immediate. So we define $m=\#C_{\sigma_0}(\mathbf{C})\cap\mathbf{T}\geq 1$.

By symmetry it suffices to prove the lemma for points $x=(x_1,\ldots,x_N)$ as in the assertion for which $d=[F(x_1):F]$ is maximal among $[F(x_1):F],\ldots,[F(x_N):F]$. So $[F(x):F]\leq d^N$ and the hypothesis on $[F(x):F]$ yields $d\geq 2m$.

We fix $\delta\in(0,1)$ with

$$-\log\delta = 2[F:\mathbf{Q}]^2m^2(4B+\log 2). \tag{16}$$

We take $\epsilon>0$ such that if $(x_1',\ldots,x_N')\in C_{\sigma_0}(\mathbf{C})$ and $\|L(x')\|<\epsilon$ then $|x_1'-t|<\delta/2$ for some $t\in\mathbf{C}$ appearing as a first coordinate of a point in $C_{\sigma_0}(\mathbf{C})\cap\mathbf{T}$. The number of such values t is at most m.

Let us suppose that $\|L(\sigma(x))\|<\epsilon$ for all σ as in the hypothesis. This will lead to a contradiction.

By the Pigeonhole Principle there is $t\in\mathbf{C}$ and a set Σ of at least $d/m\geq 2$ embeddings $\sigma:F(x_1)\to\mathbf{C}$ extending σ_0 such that $|\sigma(x_1)-t|<\delta/2$. Then $|\sigma(x_1)-\sigma'(x_1)|<\delta$ for two such embeddings.

The absolute value of the discriminant of the minimal polynomial of x_1 is a positive integer. Its logarithm is non-negative and hence

$$0\leq 2[\mathbf{Q}(x_1):\mathbf{Q}]^2h(x_1)+\sum_{\sigma\neq\sigma'}\log|\sigma(x_1)-\sigma'(x_1)|$$

where σ,σ' run over all embeddings $\mathbf{Q}(x_1)\to\mathbf{C}$. We note that $h(x_1)\leq h(x)\leq B$. Thus

$$0\leq 2[F(x_1):\mathbf{Q}(x_1)]^2[\mathbf{Q}(x_1):\mathbf{Q}]^2h(x_1)+\mathcal{D}\leq 2d^2[F:\mathbf{Q}]^2B+\mathcal{D} \tag{17}$$

with $\mathcal{D}=\sum_{\sigma(x_1)\neq\sigma'(x_1)}\log|\sigma(x_1)-\sigma'(x_1)|$ where the sum is now over all complex embeddings of $F(x_1)$.

Two distinct elements of Σ take different values at x_1. Using $\log \delta < 0$ we may bound

$$\mathcal{D} < \frac{d}{m}\left(\frac{d}{m} - 1\right)\log \delta + \sum_{\substack{\sigma(x_1) \neq \sigma'(x_1) \\ \sigma \notin \Sigma \text{ or } \sigma' \notin \Sigma}} \log|\sigma(x_1) - \sigma'(x_1)|.$$

Recall that $d/m \geq 2$. This yields $d/m - 1 \geq d/(2m)$ and

$$\mathcal{D} < \frac{d^2}{2m^2}\log \delta + \sum_{\sigma,\sigma'} \log(2\max\{1, |\sigma(x_1)|\}\max\{1, |\sigma'(x_1)|\}).$$

The definition of the height implies

$$\mathcal{D} < \frac{d^2}{2m^2}\log \delta + [F(x_1) : \mathbf{Q}]^2(2h(x_1) + \log 2) \leq \frac{d^2}{2m^2}\log \delta + d^2[F : \mathbf{Q}]^2(2B + \log 2)$$

Combining this bound with (17) and multiplying by $2m^2/d^2$ yields

$$-\log \delta < 4m^2[F : \mathbf{Q}]^2 B + 2m^2[F : \mathbf{Q}]^2(2B + \log 2) = 2[F : \mathbf{Q}]^2 m^2(4B + \log 2)$$

which contradicts (16). $\square$

We need a well-known preparatory lemma. For any integer n we let $[n] : \mathbf{G}_m^N \to \mathbf{G}_m^N$ denote the n-th power homomorphism.

Lemma 5. *Let $C \subset \mathbf{G}_m^N$ be an irreducible algebraic curve defined over $\mathbf{C}$. If C is not a coset, $n \geq 2$ is an integer and $x \in \mathbf{G}_m^N(\mathbf{C})$, then $x[n](C) \cap C$ is finite.*

Proof. This follows for example from Hindry's lemme 10 [9]. $\square$

We use Rémond's toric version of an inequality of Vojta in the next lemma.

Lemma 6. *Suppose C is not a coset. There exists a constant $B \in \mathbf{R}$ such that if $n \geq 2$ is an integer and $x \in C(\overline{\mathbf{Q}})$ with $x^n \in C(\overline{\mathbf{Q}})$, then $h(x) \leq B$.*

Proof. For such n sufficiently large with respect to C we may invoke Rémond's théorème 3.1 [15]. In its notation we take to $x_2 = x^n$ and $x_1 = x$. Our result follows quickly from the observation that Rémond's angular distance $\widehat{(x_1, x_2)}$ vanishes. The finitely many integers $n \geq 2$ not covered by Rémond's Theorem can be treated with Lemma 5. $\square$

Proposition 7. *Suppose C is as in Lemma 4. There exists a constant $c > 0$ with the following property. If $x \in C(\overline{\mathbf{Q}})$ is of infinite order and $x^n \in C(\overline{\mathbf{Q}})$ for some $n \geq 2$, then*

$$[F(x) : F] \geq cn^{1/7}.$$

Proof. There exists σ_0 as in Lemma 4. Lemma 6 implies that x has height bounded solely in terms of C. So by Northcott's Theorem, there are only finitely many x of degree at most $(2\#C_{\sigma_0}(\mathbf{C}) \cap \mathbf{T})^N$. But for a fixed x of infinite order the set $\{n \in \mathbf{N};\ x^n \in C(\overline{\mathbf{Q}})\}$ is finite by a result of Lang, cf. Chapter 8, Theorem 3.2 [10]. Here we need that C is not a coset. Thus for x of degree at most $(2\#C_{\sigma_0}(\mathbf{C}) \cap \mathbf{T})^N$, there is an upper bound on the n appearing in the statement of the lemma; so for these x the degree lower bound in the assertion is satisfied if c is sufficiently small.

So we need only consider points x with $[F(x) : F] \geq (2\#C_{\sigma_0}(\mathbf{C}) \cap \mathbf{T})^N$. In particular, the degree lower bound in Lemma 4 is satisfied.

Suppose $\epsilon > 0$ is as in said lemma. Recall that it is independent of x. Now we fix $\sigma : F(x) \to \mathbf{C}$ extending σ_0 such that $\|L(\sigma(x))\| \geq \epsilon$.

After decreasing ϵ we may assume $\|L(\sigma(x'))\| \geq \epsilon$ where x' is the projection of x to two distinct coordinates of $\mathbf{G}_m^N$. This projection lies on C', the Zariski closure of the the projection of C to $\mathbf{G}_m^2$. We remark that C' is an irreducible algebraic curve and not a coset. Applying Lemma 3(i) to C', inequality (10) yields

$$\frac{n}{\log n}\epsilon \leq \frac{n}{\log n}\|L(\sigma(x'))\| \leq c[F(x') : F]^6 \leq c[F(x) : F]^6,$$

with $c > 0$ independent of x and n. The proposition follows after adjusting c. □

Lemma 8. *Suppose that C is not a torsion coset of $\mathbf{G}_m^N$. There exists $\epsilon > 0$ with the following property. If $x = (x_1, \ldots, x_N) \in C(\overline{\mathbf{Q}})$ has infinite order and if all x_i are algebraic integers there is an embedding $\sigma : F(x) \to \mathbf{C}$ with*

$$\|L(\sigma(x))\| \geq \epsilon.$$

Proof. The Bogomolov Conjecture, proved in this case by Zhang [19], implies that there is $\epsilon > 0$ such that any algebraic point of C of infinite order has height at least ϵ. If x is as in the hypothesis then only the Archimedean places contribute to the height of x. The lemma follows easily after possibly modifying ϵ. □

Proposition 9. *Suppose C is as in Lemma 8. Let S be a finite set of rational primes with $\inf S$ sufficiently large with respect to C. There exists a constant $c > 0$ with the following property. If $x = (x_1, \ldots, x_N) \in C(\overline{\mathbf{Q}})$ is S-integral and of infinite order with $x^n \in C(\overline{\mathbf{Q}})$ for some $n \geq 2$, then*

$$[F(x) : F] \geq cn^{1/9}.$$

Proof. The proposition follows along the lines of the proof of Proposition 7. Indeed, if all x_i are algebraic integers, then Lemmas 3 and 8 do the trick. Otherwise there is a number field and a place v with residue characteristic in S such that $|x_i|_v > 1$ for some i. By decreasing c we may suppose that said characteristic is large enough in order to apply part (ii) of Lemma 3 to a suitable projection of C. Inequality (11) is stronger than our claim. □

6. O-MINIMALITY

We refer to [16] for the essentials on o-minimal structures. We will work with the structure $\mathbf{R}_{\exp,\sin_|} = \left\langle \mathbf{R}; +, \cdot, \exp, \sin|_{[0,2\pi)} \right\rangle$ generated as a structure over the real field by the real exponential function and restricted sine. This structure is o-minimal, by a theorem of Wilkie [17, Example B]; its o-minimality also follows from the well-known stronger result that $\mathbf{R}_{\mathrm{an},\exp}$ is o-minimal.

We will call a subset of $\mathbf{R}^m$ definable if it is definable in $\mathbf{R}_{\exp,\sin_|}$. We identify $\mathbf{C}$ with $\mathbf{R}^2$ by identifying a complex number with the pair consisting of its real and imaginary parts.

The complex exponential function $\exp : \mathbf{C}^N \to (\mathbf{C}^\times)^N$ restricted to the fundamental domain $\mathcal{F} = (\mathbf{R} + [0, 2\pi)i)^N$ is definable. Hence

$$X = \{(n, z, k) \in \mathbf{R}\times\mathcal{F}\times\mathbf{R}^N;\ \exp(z) \in C(\mathbf{C}),\ nz-2\pi ik \in \mathcal{F},\ \exp(nz-2\pi ik) \in C(\mathbf{C})\},$$

is also definable, as is its projection $Z \subset \mathbf{R}\times\mathbf{R}^N$ to the first and the last N coordinates.

We will treat X and Z as definable families parametrized by the parameter $n \in \mathbf{R}$. As is usual $X_n \subset \mathcal{F} \times \mathbf{R}^N$ and $Z_n \subset \mathbf{R}^N$ denote the respective fibers. The latter is the projection of X_n to the final N coordinates.

We will be interested in integral n. We will show that Z_n contains no semi-algebraic curves if $n \geq 2$.

The main tool in studying the semi-algebraic curves contained in fibers of Z is Ax's Theorem. We state only a special case. Let $\Delta = \{t \in \mathbf{C};\ |t| < 1\}$.

Theorem 3 (Ax)**.** *Suppose $\gamma_1, \ldots, \gamma_N : \Delta \to \mathbf{C}^N$ are holomorphic functions for which $\gamma_1 - \gamma_1(0), \ldots, \gamma_N - \gamma_N(0)$ are $\mathbf{Z}$-linearly independent. Then*

$$\operatorname{trdeg} \mathbf{C}(\gamma_1, \ldots, \gamma_N, \exp \circ \gamma_1, \ldots, \exp \circ \gamma_N)/\mathbf{C} \geq N + 1.$$

Proof. By hypothesis, not all γ_i are constant. So the claim follows directly from the one variable case of [1, Corollary 2]. □

Proposition 10. *We assume that $N \geq 3$ and that C is not contained in a proper coset of $\mathbf{G}_m^N$. If $n \geq 2$ is integral, then Z_n does not contain a semi-algebraic curve.*

Proof. Let us assume the contrary and suppose that Z_n contains a semi-algebraic curve S. So there is a semi-algebraic and non-constant map $\gamma : (-1, 1) \to S$. After reparametrizing we may suppose that the coordinates $\gamma_1, \ldots, \gamma_N$ of γ extend to a holomorphic function defined on Δ with values in $\mathbf{C}^N$ and with $\operatorname{trdeg}(\mathbf{C}(\gamma)/\mathbf{C}) = 1$.

"Definable Choice" provides us with a definable map $\theta : (-1, 1) \to \mathcal{F}$ such that

$$(\theta(t), \gamma(t)) \in X_n \quad \text{for all} \quad t \in (-1, 1).$$

Definable sets in $\mathbf{R}_{\exp,\sin_|}$ admit a decomposition into analytic cells. So the function θ is real analytic in a neighborhood of some point of $(-1, 1)$. At this point the real- and imaginary parts of all coordinates of θ have a Taylor expansion. Each of these $2N$ functions admits a holomorphic continuation in a neighborhood of said point. By taking appropriate linear combinations after possibly reparametrizing, we find that θ continues to a holomorphic function $\Delta \to \mathbf{C}^N$. The image of $\exp \circ \theta : \Delta \to \mathbf{G}_m^N(\mathbf{C})$ is still contained in $C(\mathbf{C})$ by analyticity.

(Although we choose not to present it this way, readers versed in model theory may find it helpful to consider $\gamma(t)$ and $\theta(t)$ as points in an elementary extension ${}^*\mathbf{R} = \operatorname{dcl}(\mathbf{R}, t)$, with $\gamma(t)$ generic on S over $\mathbf{R}$ and $\theta(t)$ a witness point in X_n. In this view, we can directly apply [1, Theorem 3] via a technique due to Wilkie, considering ${}^*\mathbf{C} = {}^*\mathbf{R} + i{}^*\mathbf{R}$ as a differential field with $\delta(f(t)) := f'(t)$ for f a function defined over $\mathbf{R}$.)

We consider the morphism $\varphi : \mathbf{G}_m^N \times \mathbf{G}_m^N \to \mathbf{G}_m^N$ defined by $\varphi(x, y) = x^{-n}y$. The Zariski closure of $\varphi(C \times C)$ has dimension at most 2. The Zariski closure Y of image of $t \mapsto \exp(-2\pi i \gamma(t))$ is contained in $\varphi(C \times C)$ and hence has dimension at most 2. We remark that Y is irreducible.

Since $N + 1 > 1 + 2$, Ax's Theorem implies that the co-ordinates of γ are $\mathbf{Z}$-linearly dependent modulo constants, and so the variety Y is contained in a proper coset.

If $\dim Y = 2$ then $\varphi(C \times C)$ is contained in a proper coset. The same then holds true for $C \times C$ and also C. This contradicts our hypothesis and so $\dim Y \leq 1$.

So if $1 \leq i, j \leq N$ then

$$\operatorname{trdeg} \mathbf{C}(\gamma_i, \gamma_j, \exp \circ \gamma_i, \exp \circ \gamma_j)/\, \mathbf{C} \leq \operatorname{trdeg} \mathbf{C}(\gamma, \exp \circ \gamma)/\mathbf{C} \leq 2$$

and so γ_i and γ_j are $\mathbf{Z}$-linearly dependent modulo constants by Ax's Theorem. So Y is itself a coset, and there is a surjective homomorphism of algebraic groups $\phi : \mathbf{G}_m^N \to \mathbf{G}_m^{N-1}$ that is constant on Y.

It is convenient to write C' for the Zariski closure of $\phi(C)$. For $t \in \Delta$ we have $\phi(\exp(n\theta(t) - 2\pi i\gamma(t))) \in C'(\mathbf{C})$. Moreover,

$$\phi(\exp(n\theta(t) - 2\pi i\gamma(t))) = x_0\phi(e^{\theta(t)})^n \in C'(\mathbf{C}) \cap x_0[n](C'(\mathbf{C}))$$

where $x_0 = \phi(\exp(-2\pi i\gamma(t)))$ is independent of t.

If $t \mapsto \phi(e^{\theta(t)})^n$ is non-constant on Δ, then it takes infinitely many values. In this case $C' \cap x_0[n](C')$ is infinite. By comparing dimension we find $C' = x_0[n](C')$ since both sides are irreducible curves. By Lemma 5 the curve C' is a coset. Therefore, C is contained in a proper coset of $\mathbf{G}_m^N$ and we have a contradiction.

So $t \mapsto \phi(\exp(n\theta(t)))$ and even $t \mapsto \theta(t)$ must be constant. So $\operatorname{trdeg} \mathbf{C}(n\theta - 2\pi i\gamma)/\mathbf{C} = \operatorname{trdeg} \mathbf{C}(\gamma)/\mathbf{C} = 1$. As we deduced from Ax's Theorem, the components of γ are $\mathbf{Z}$-linearly dependent modulo constants. But γ is non-constant and holomorphic, so $\exp(n\theta - 2\pi i\gamma)$ takes infinitely many values in $C(\mathbf{C})$. It follows that C is contained in a proper coset and this contradicts the hypothesis. $\square$

7. Proof of the Theorems

We will prove Theorems 1 and 2 simultaneously. The only difference in treating these two cases is if we will refer to Proposition 7 or 9.

Suppose that C is as in the hypothesis. We first reduce to the case where C is not contained in a proper coset. Otherwise there is a coset yH with $C \subset yH$ where $H \subsetneq \mathbf{G}_m^n$ is a connected algebraic subgroup. If $x \in C(\overline{\mathbf{Q}})$ and $x^n \in C(\overline{\mathbf{Q}})$ for some $n \geq 2$, then $x \in yH \cap y^nH$ and so $yH = y^nH$ which yields $y^{n-1} \in H$. Therefore, yH is a proper torsion coset containing C, contradicting the hypothesis.

By the Manin-Mumford Conjecture for curves in $\mathbf{G}_m^N$ there are only finitely many points on C of finite order. Hence we must prove that there are only finitely many non-torsion $x \in C(\overline{\mathbf{Q}})$ with $x^n \in C(\overline{\mathbf{Q}})$ for some $n \geq 2$. For a fixed n there are only finitely many such points by Lemma 5. We will prove the theorem by deriving a contradiction for all sufficiently large n.

By Proposition 7 or 9, there are at least $c_1 n^{1/9}$ conjugates $x_1, \ldots, x_M$ of x over F; here and below c_1, c_2, c_3 are positive constants that do not depend on n or x.

These conjugates and their n-th powers are points on $C(\overline{\mathbf{Q}})$. For each x_j there is $z_j \in \mathcal{F}$ and $k_j \in \mathbf{Z}^N$ with $\exp(z_j) = x_j$ and $nz_j - 2\pi i k_j \in \mathcal{F}$. Then

$$(z_j, k_j) \in X_n \quad \text{and} \quad k_j \in Z_n \cap \mathbf{Z}^N \quad \text{for all} \quad 1 \leq j \leq M \tag{18}$$

where X and Z are as in Section 6.

The fiber Z_n does not contain a real semi-algebraic curve by Proposition 10. So we can use the Pila-Wilkie Theorem [13] to bound from above the number of integral points of bounded height on Z_n. As this result is uniform in families we find a constant c_2 independent of n such that

$$\#\{k \in Z_n \cap \mathbf{Z}^N;\ H(k) \leq n\} \leq c_2 n^{1/10}; \tag{19}$$

we recall that the height $H(k)$ was defined in Section 2. Of course, the exponent $1/10$ can be replaced by any positive constant at the cost of increasing c_2.

We proceed to show that k_j are among the elements being counted in (19). Indeed, the imaginary part of the components of z_j and $nz_j - 2\pi i k_j$ lie in $[0, 2\pi)$. So the components of k_j are in $[0, n)$. Because $H(k_j)$ is the largest modulus of a component we find $H(k_j) \le n$.

We already know that there at least $c_1 n^{1/10}$ distinct z_j. But we require a lower bound for the number of k_j. By a basic uniformity property of o-minimal structures the number of connected components of the fiber

$$X_{n,k_j} = \{z \in \mathcal{F};\ (z, k_j) \in X_n\}$$

is bounded from above by a constant c_3 that does not dependent on k_j or n.

We claim that each X_{n,k_j} is finite. If this is not the case there would be infinitely many $x \in C(\mathbf{C})$ with $x^n \in C(\mathbf{C})$. This is impossible by Lemma 5.

So $\# X_{n,k_j} \le c_3$ and the number of distinct k_j is at least $\frac{c_1}{c_3} n^{1/10}$. This lower bound contradicts (19) for n sufficiently large. $\square$

References

1. J. Ax, *On Schanuel's conjectures*, Ann. of Math. (2) **93** (1971), 252–268.
2. A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19–62.
3. E. Bombieri, D.W. Masser, and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Internat. Math. Res. Notices (1999), no. 20, 1119–1140.
4. Y. Bugeaud and M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory **61** (1996), no. 2, 311–342.
5. P. Corvaja, D. Masser, and U. Zannier, *Sharpening 'Manin-Mumford' for certain algebraic groups of dimension* 2, To appear in Enseign. Math.
6. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401.
7. A.J. Engler and A. Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.
8. P. Habegger, *On the Bounded Height Conjecture*, Internat. Math. Res. Notices (2009), no. 5, 860–886.
9. M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), no. 3, 575–603.
10. S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, 1983.
11. G. Maurin, *Équations multiplicatives sur les sous-variétés des tores*, Int. Math. Res. Not. IMRN (2011), no. 23, 5259–5366.
12. J. Neukirch, *Algebraic number theory*, vol. 322, Springer-Verlag, Berlin, 1999.
13. J. Pila and A. J. Wilkie, *The rational points of a definable set*, Duke Math. J. **133** (2006), no. 3, 591–616.
14. J. Pila and U. Zannier, *Rational points in periodic analytic sets and the manin-mumford conjecture*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **19** (2008), no. 2, 149–162.
15. G. Rémond, *Sur les sous-variétés des tores*, Compositio Math. **134** (2002), no. 3, 337–366.
16. L. van den Dries, *Tame topology and o-minimal structures*, London Mathematical Society Lecture Note Series, vol. 248, Cambridge University Press, Cambridge, 1998.
17. A.J. Wilkie, *Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function*, J. Amer. Math. Soc. **9** (1996), no. 4, 1051–1094.
18. U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Mathematics Studies, vol. 181, Princeton University Press, 2012, With appendixes by David Masser.
19. S. Zhang, *Positive line bundles on arithmetic varieties*, J. Amer. Math. Soc. **8** (1995), no. 1, 187–221.

20. B. Zilber, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. (2) **65** (2002), no. 1, 27–44.

Martin Bays, McMaster University, Ontario, Canada

Philipp Habegger, Johann Wolfgang Goethe-Universität, Robert-Mayer-Str. 6-8, 60325 Frankfurt am Main, Germany, habegger@math.uni-frankfurt.de